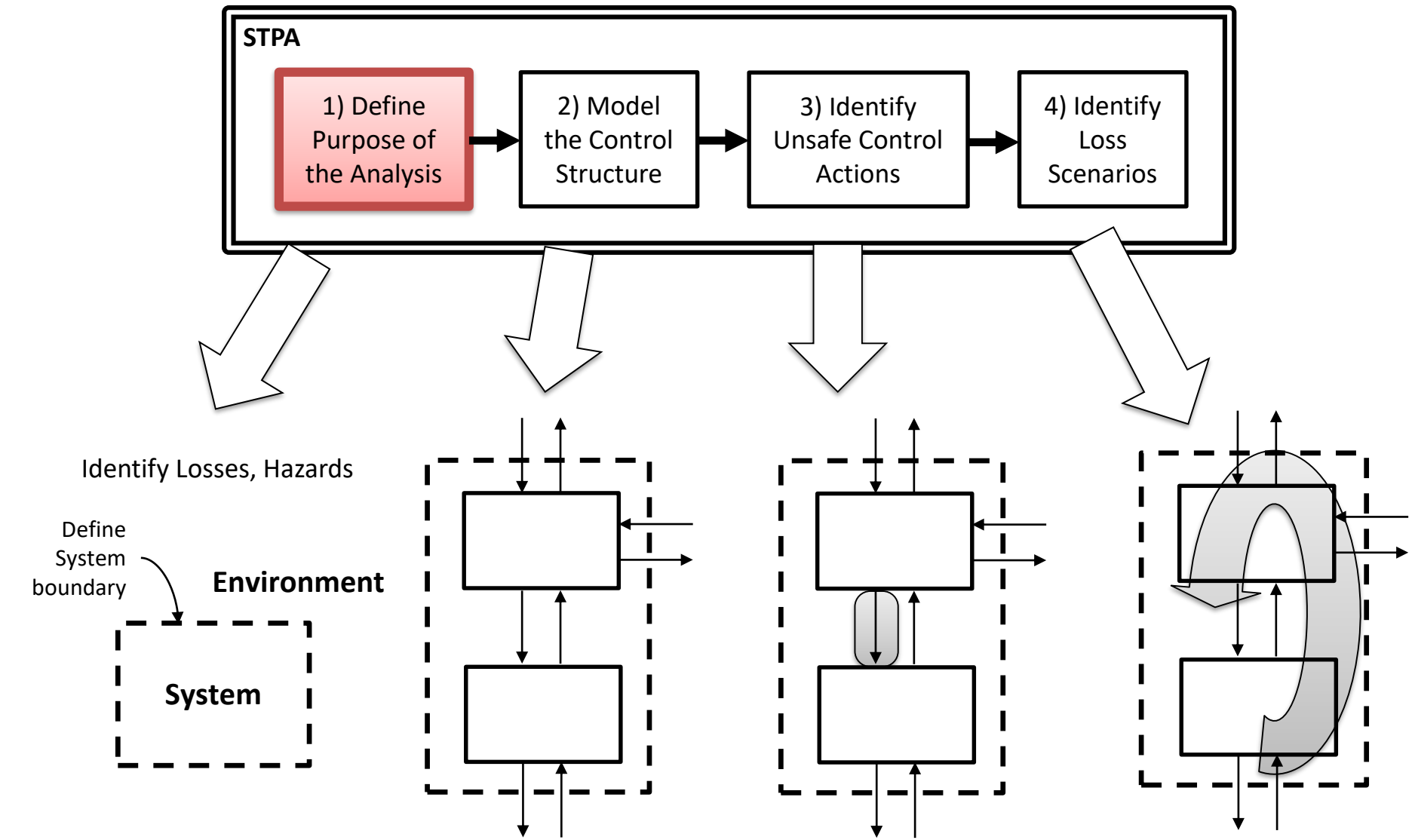
Short Exercise inspired by Tesla Autopilot

Spring 2016 Student project: Diogo Castilho, Megan France

Disclaimer

These exercises are not meant to represent a complete analysis, and they are not meant to exhaustively demonstrate STPA.

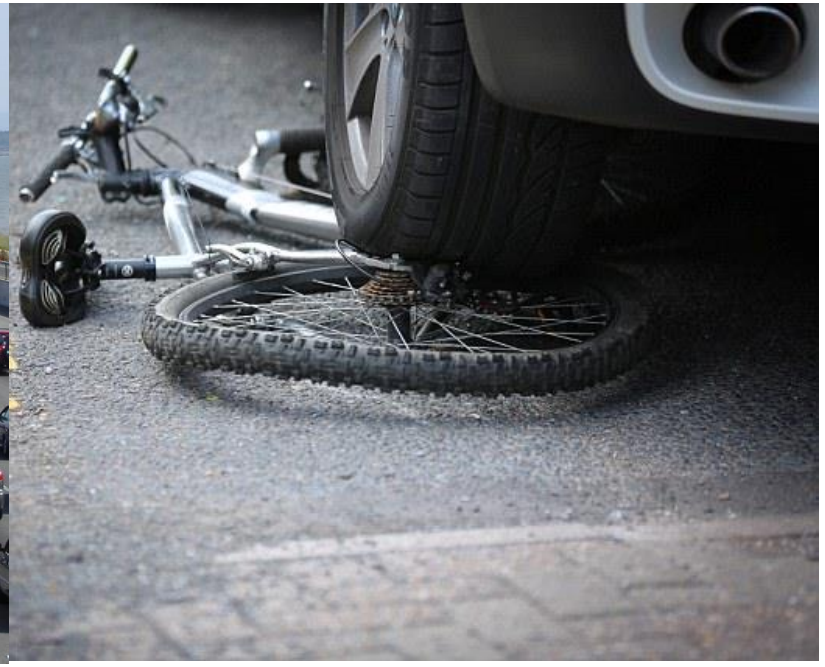
The exercises are only meant to introduce a few core concepts.

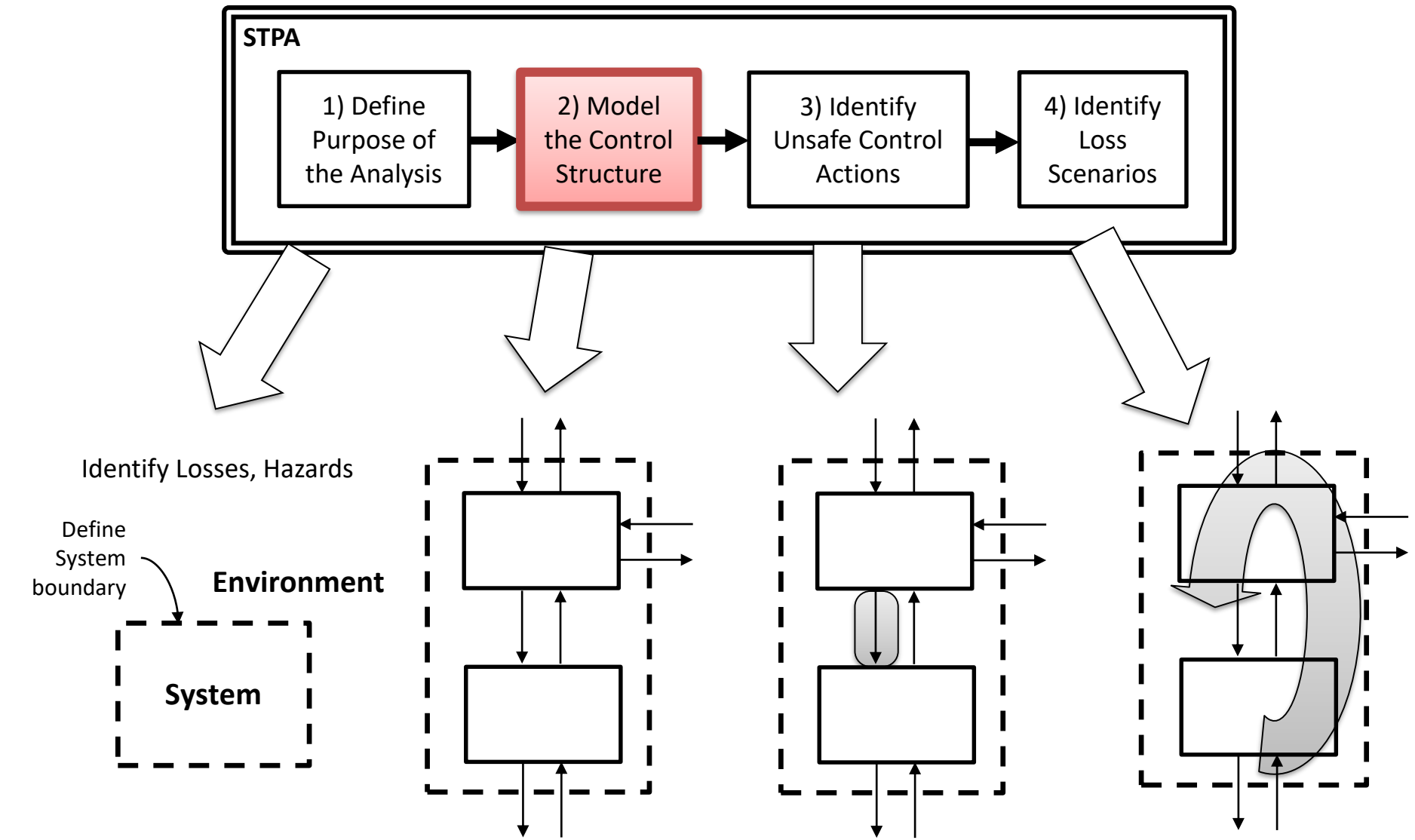


(Leveson and Thomas, 2018)

Automotive Example

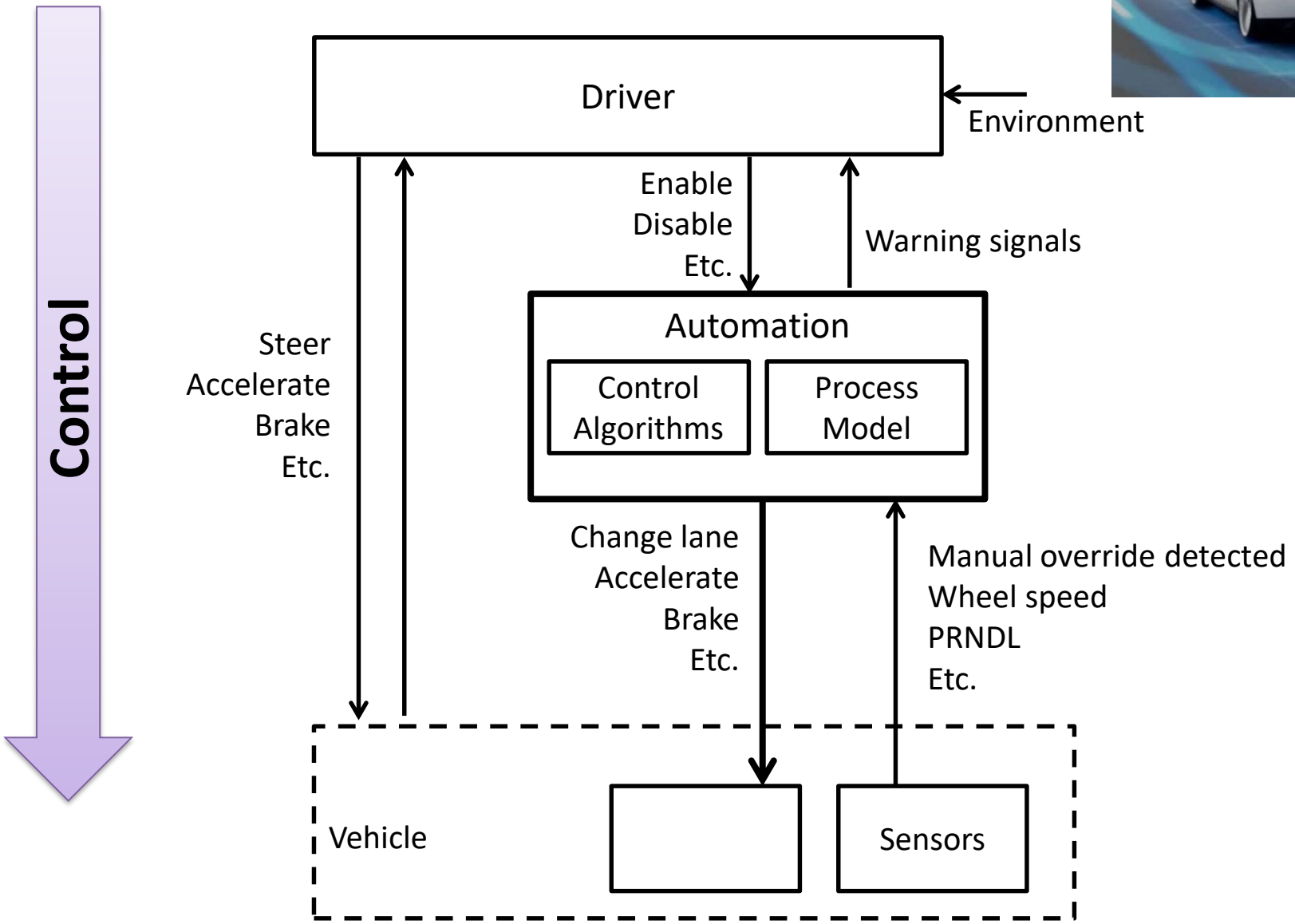
- Losses
  - L-1. Loss of life or serious injury to people
  - L-2. Damage to the vehicle or objects outside the vehicle
  - L-3: Loss of mission (transportation)
  - L-4: Loss of customer satisfaction

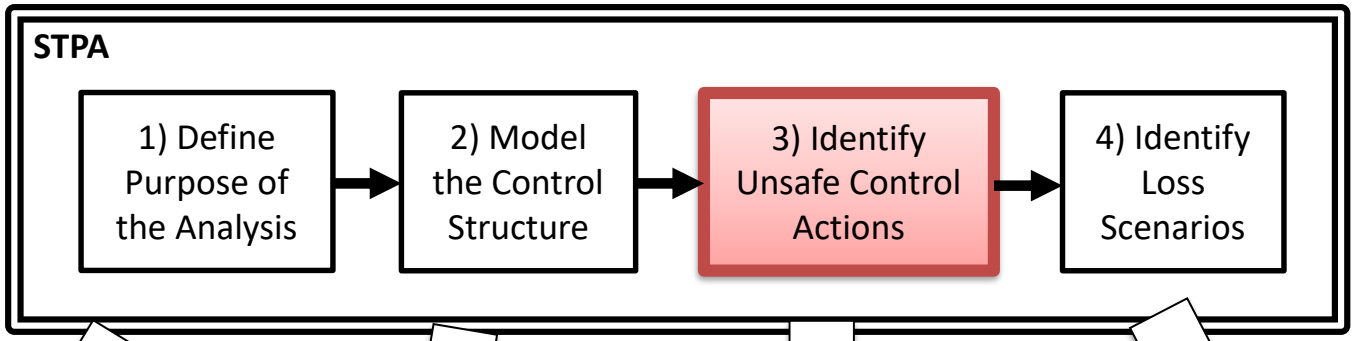




(Leveson and Thomas, 2018)

High-level Control Structure



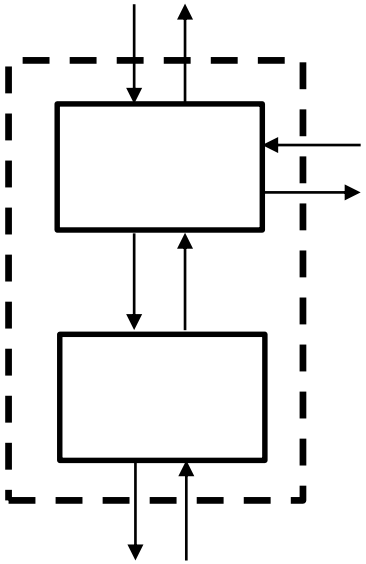


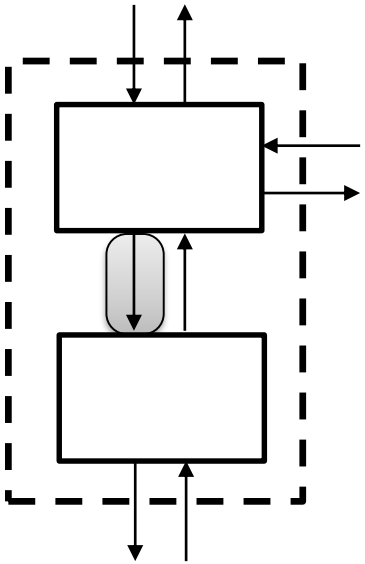
Identify Losses, Hazards

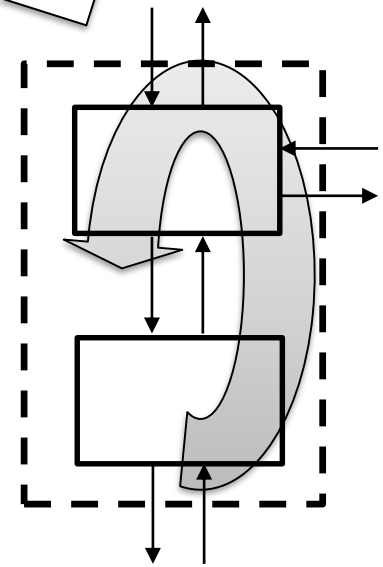
Define System boundary

Environment

System

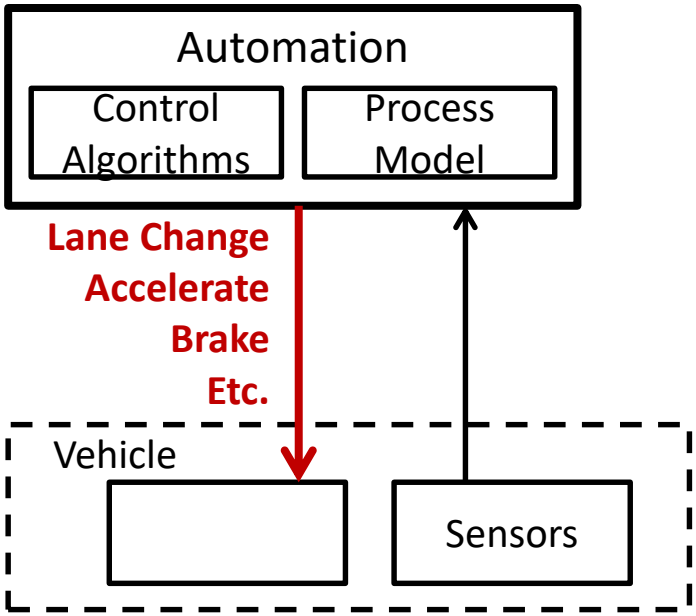






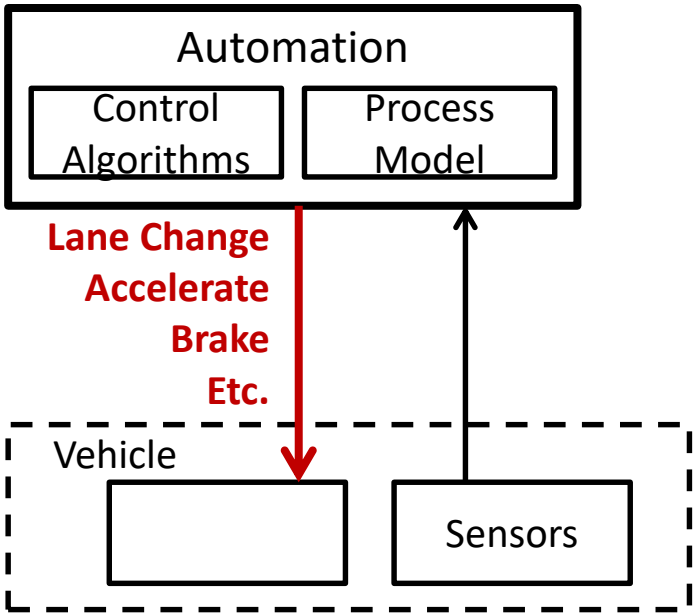
(Leveson and Thomas, 2018)

STPA: Unsafe Control Actions (UCA)



	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Brake Command	?			

STPA: Unsafe Control Actions (UCA)



Example:

“_____ _____ _____cmd when _____”

Source Controller

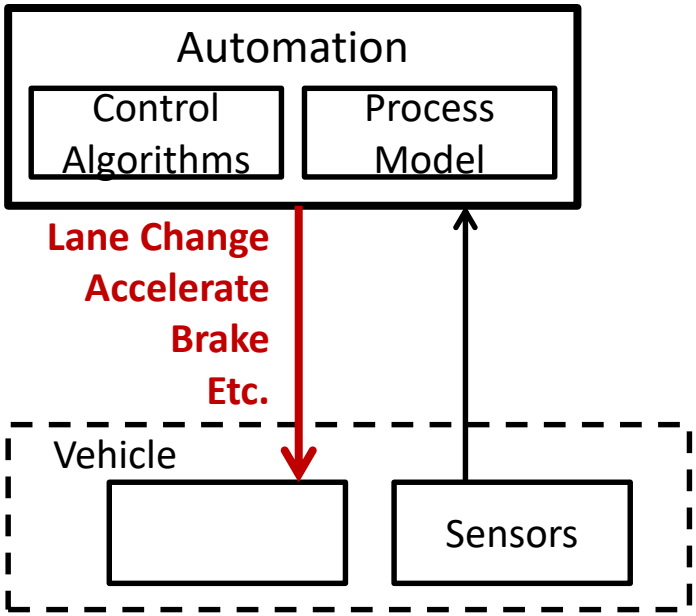
Type

Control Action

Context

	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Brake Command	?			

STPA: Unsafe Control Actions (UCA)



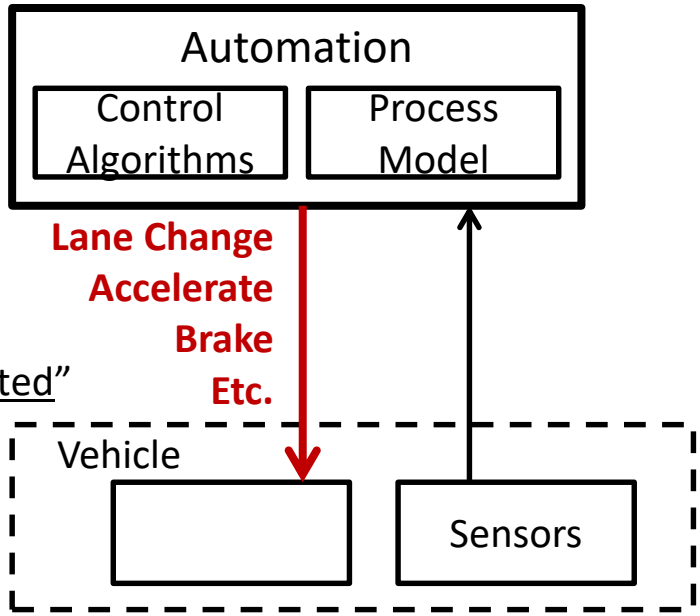
Example:

"Automation does not provide brake cmd when _____"

- Automation: Source Controller
- does not provide: Type
- brake cmd: Control Action
- _____: Context

	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Brake Command	Automation does not provide Brake cmd when _____			

STPA: Unsafe Control Actions (UCA)

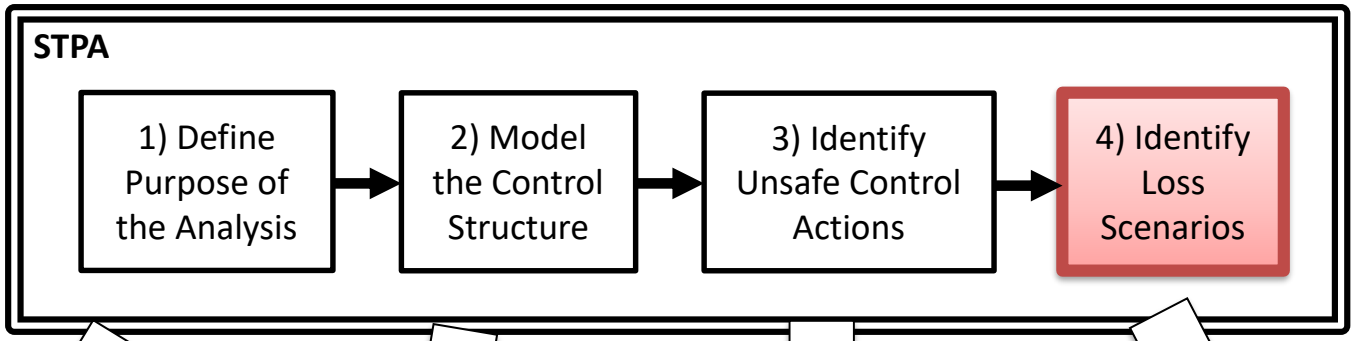


Example:

"Automation does not provide brake cmd when path is obstructed"

- Automation: Source Controller
- does not provide: Type
- brake cmd: Control Action
- path is obstructed: Context

	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Brake Command	UCA-1: Automation does not provide Brake cmd when vehicle path is obstructed [L-1,L-2]			

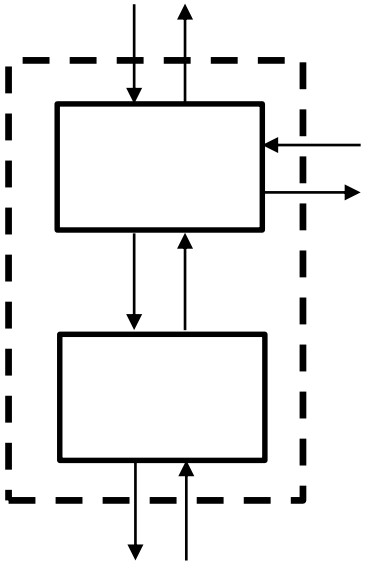


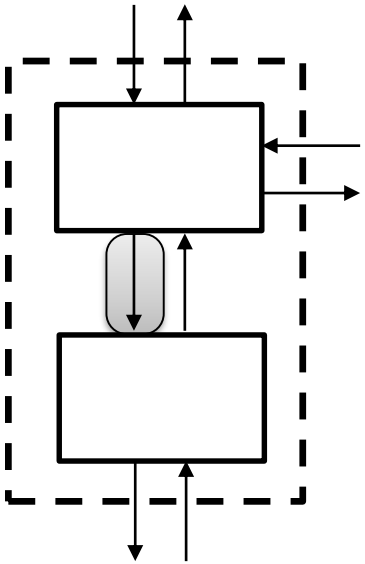
Identify Losses, Hazards

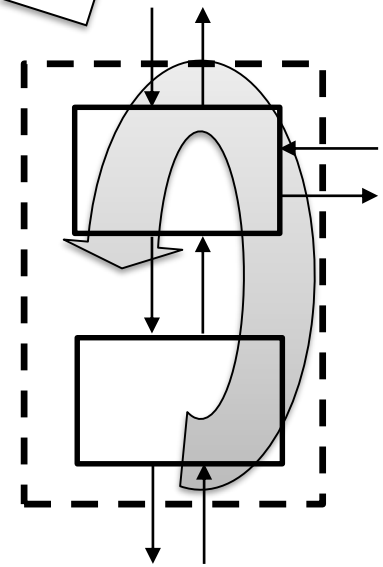
Define System boundary

Environment

System

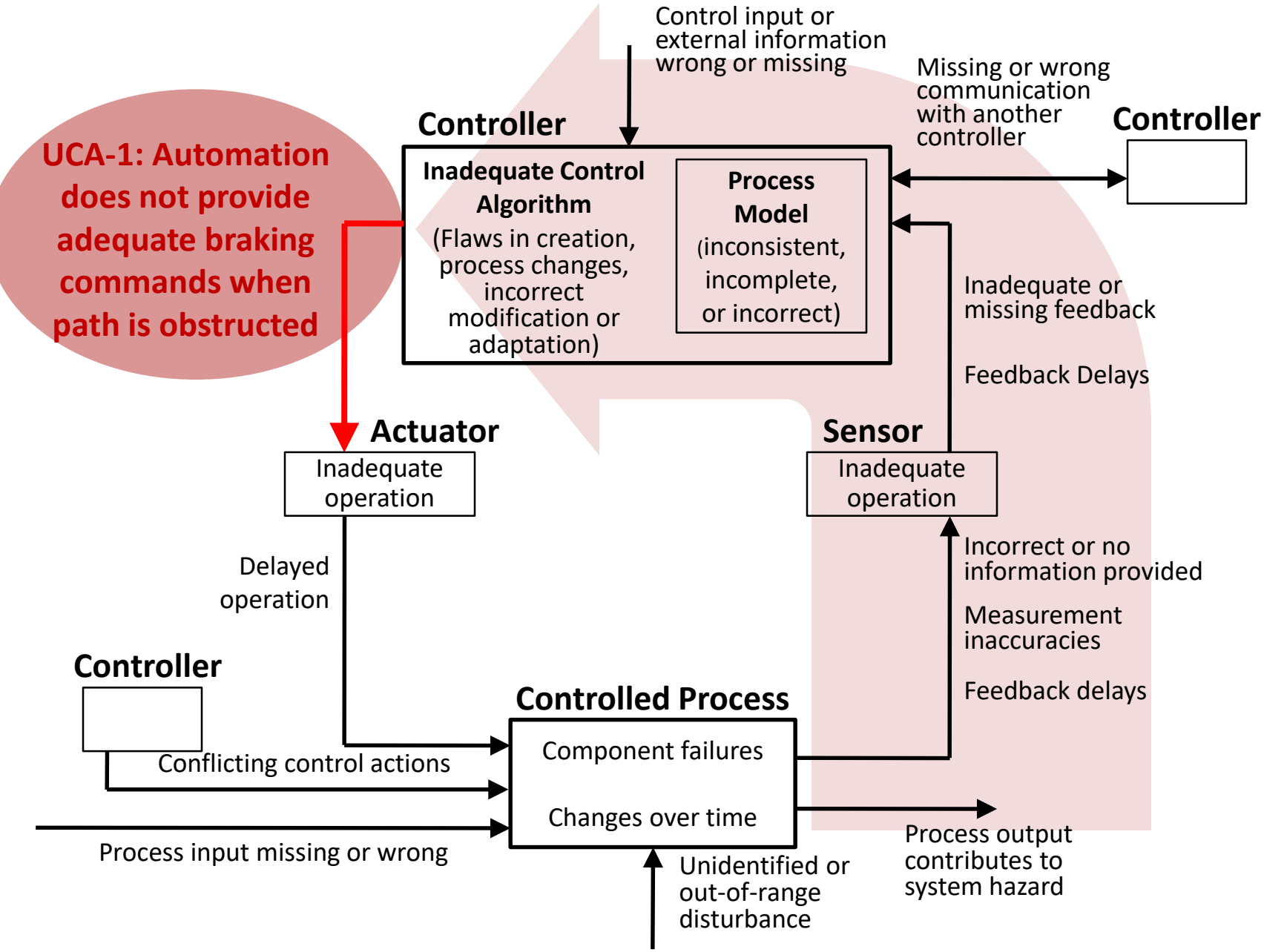




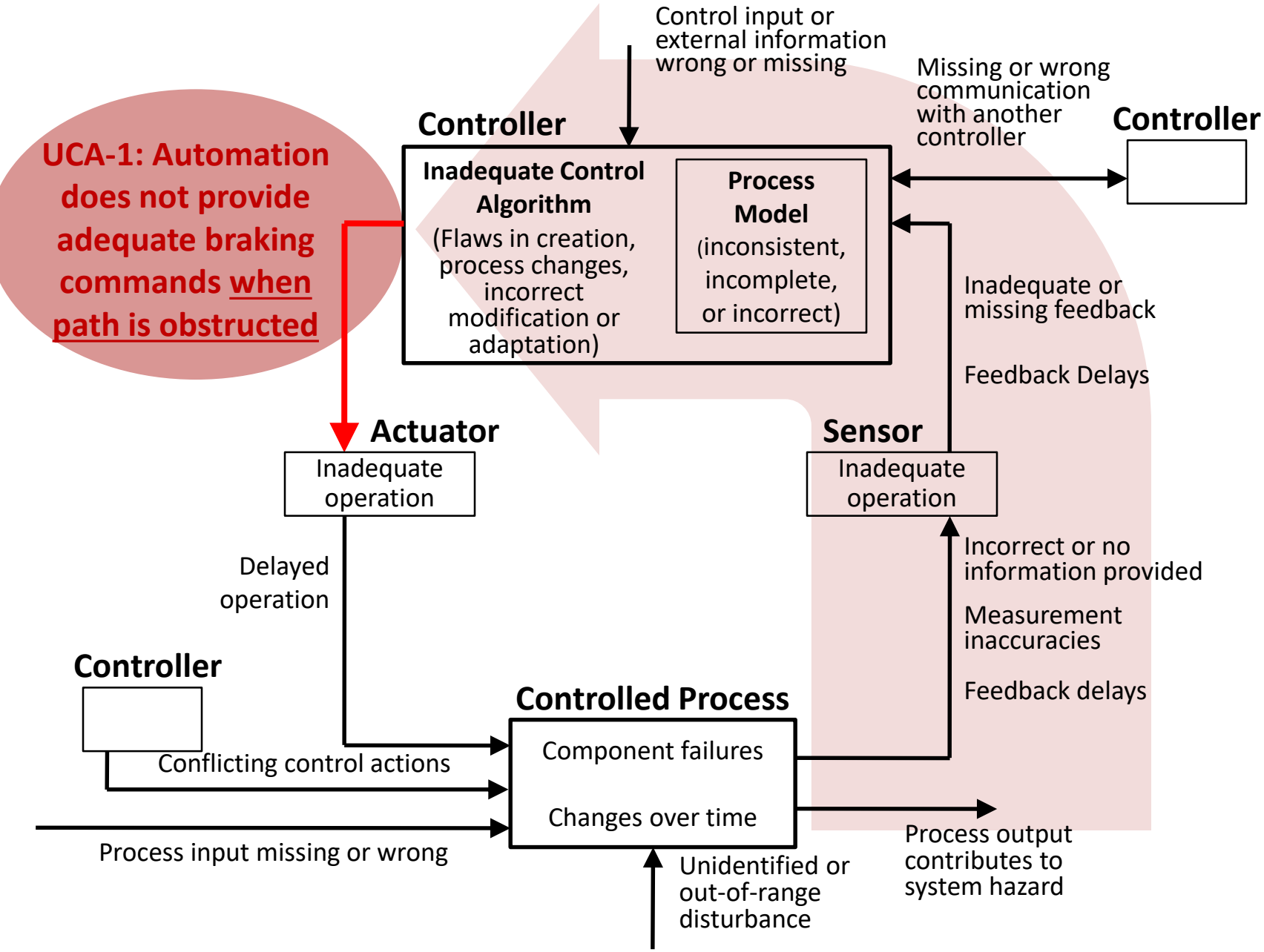


(Leveson and Thomas, 2018)

Step 4: Potential causes of UCAs

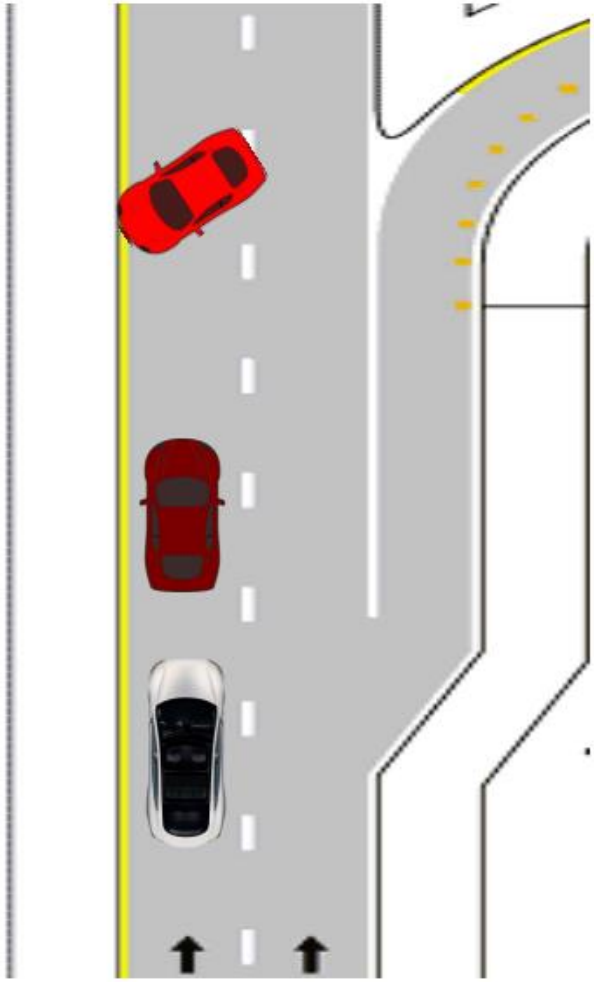


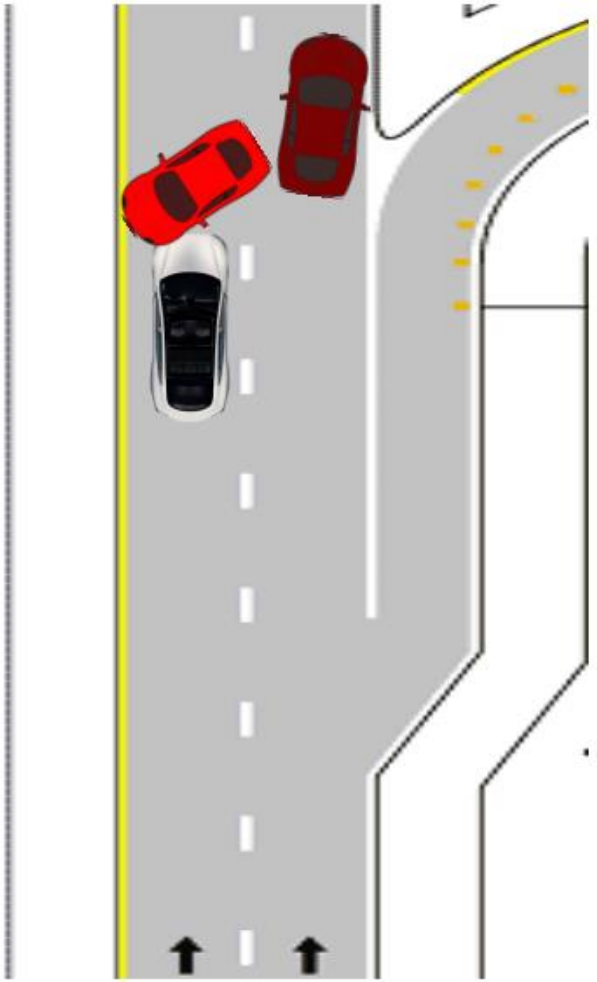
Step 4: Potential causes of UCAs



Scenario #1

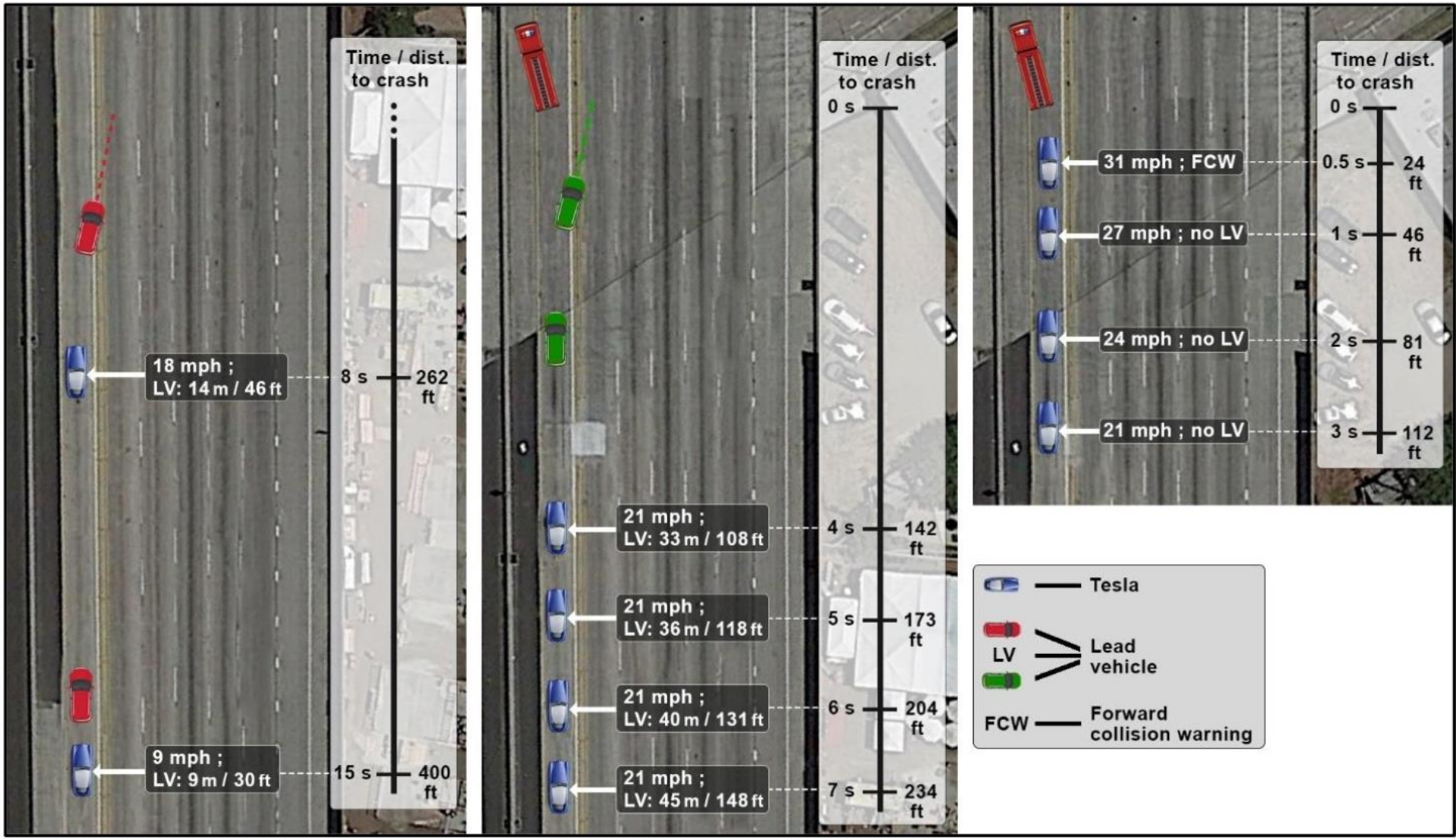
UCA-1: Autopilot does not provide adequate braking commands for obstacle ahead



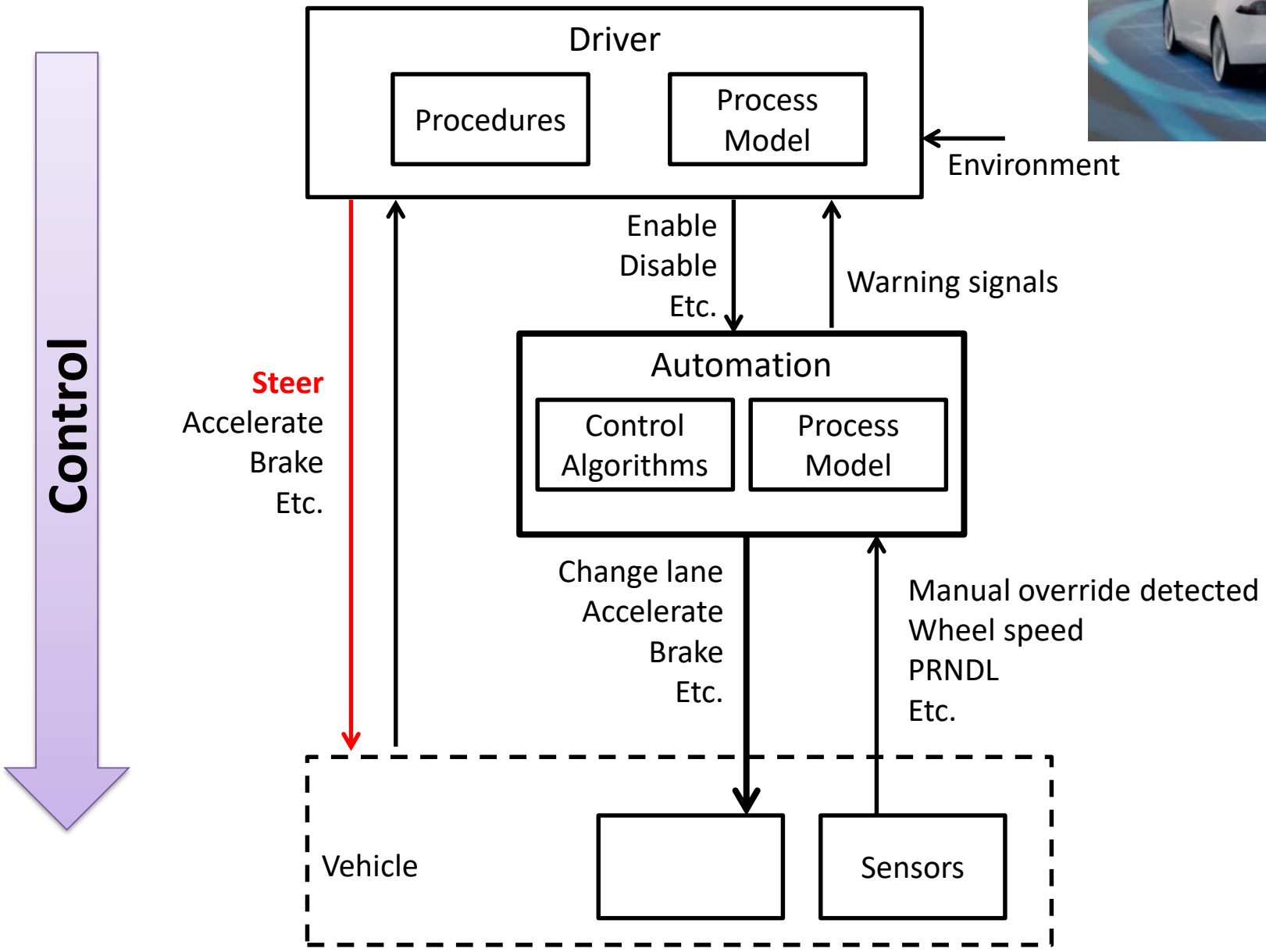


Spring 2016 Student project: Diogo Castilho, Megan France

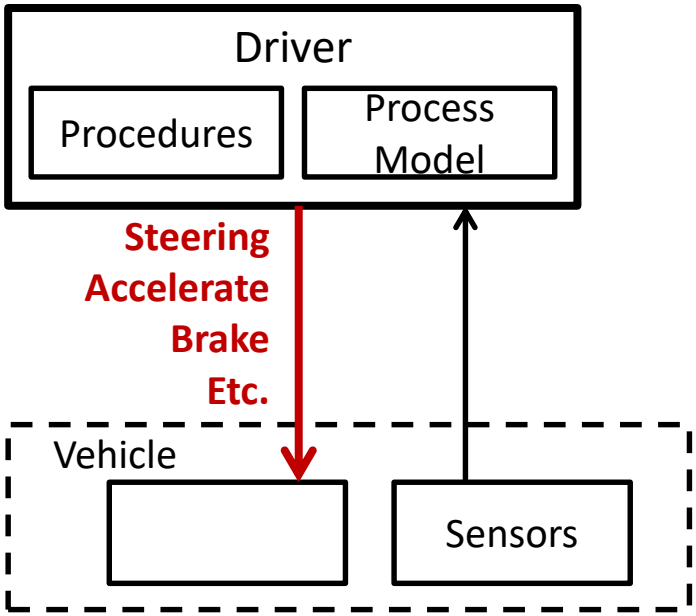
Tesla crash January 22, 2018


Time / dist. to crash
18 mph ; LV: 14 m / 46 ft
8 s
262 ft
9 mph ; LV: 9 m / 30 ft
15 s
400 ft
Time / dist. to crash
0 s
21 mph ; LV: 33 m / 108 ft
4 s
142 ft
21 mph ; LV: 36 m / 118 ft
5 s
173 ft
21 mph ; LV: 40 m / 131 ft
6 s
204 ft
21 mph ; LV: 45 m / 148 ft
7 s
234 ft
Time / dist. to crash
0 s
31 mph ; FCW
0.5 s
24 ft
27 mph ; no LV
1 s
46 ft
24 mph ; no LV
2 s
81 ft
21 mph ; no LV
3 s
112 ft
Tesla
LV
Lead vehicle
FCW
Forward collision warning

High-level Control Structure

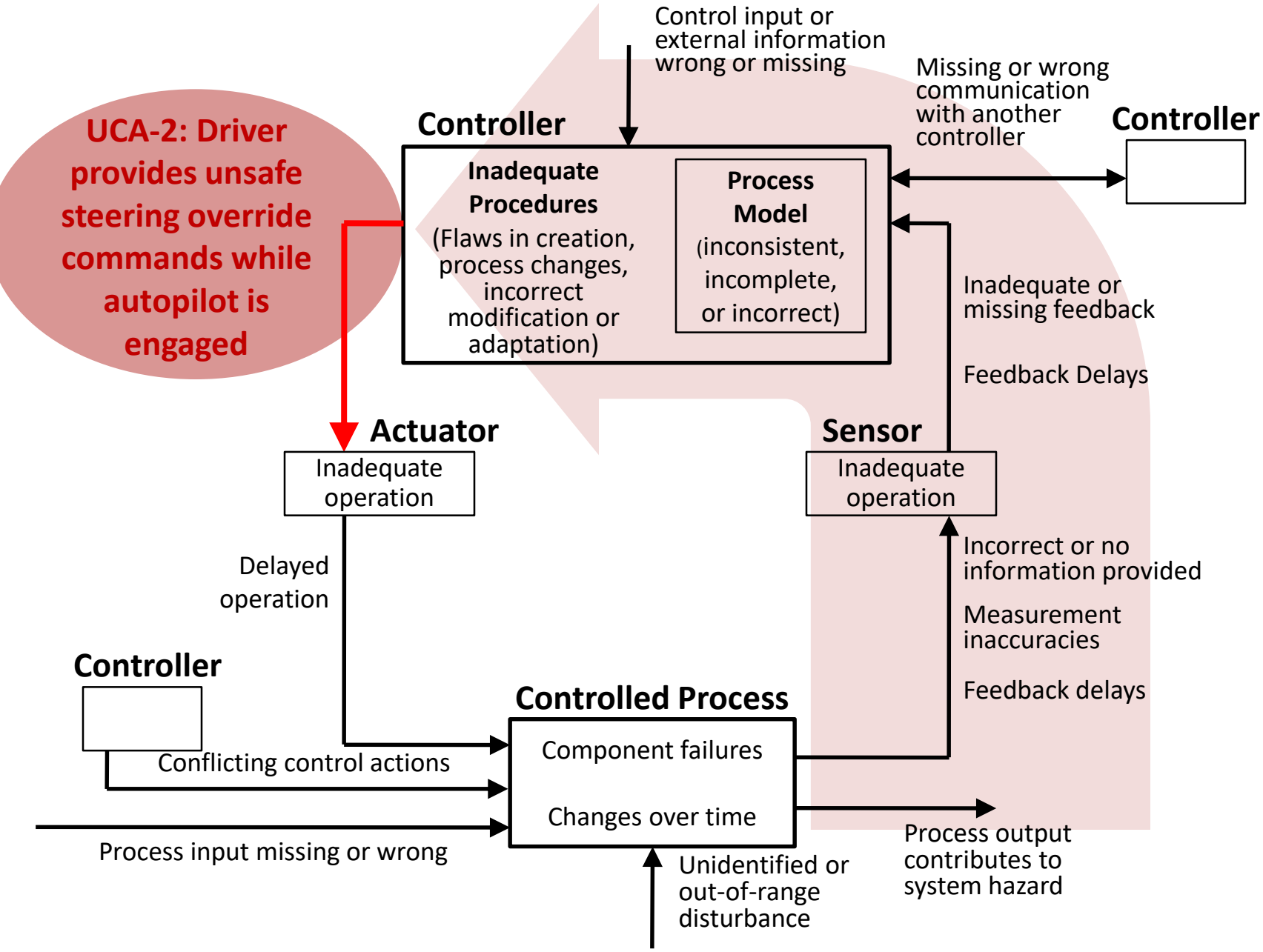


STPA: Unsafe Control Actions (UCA)



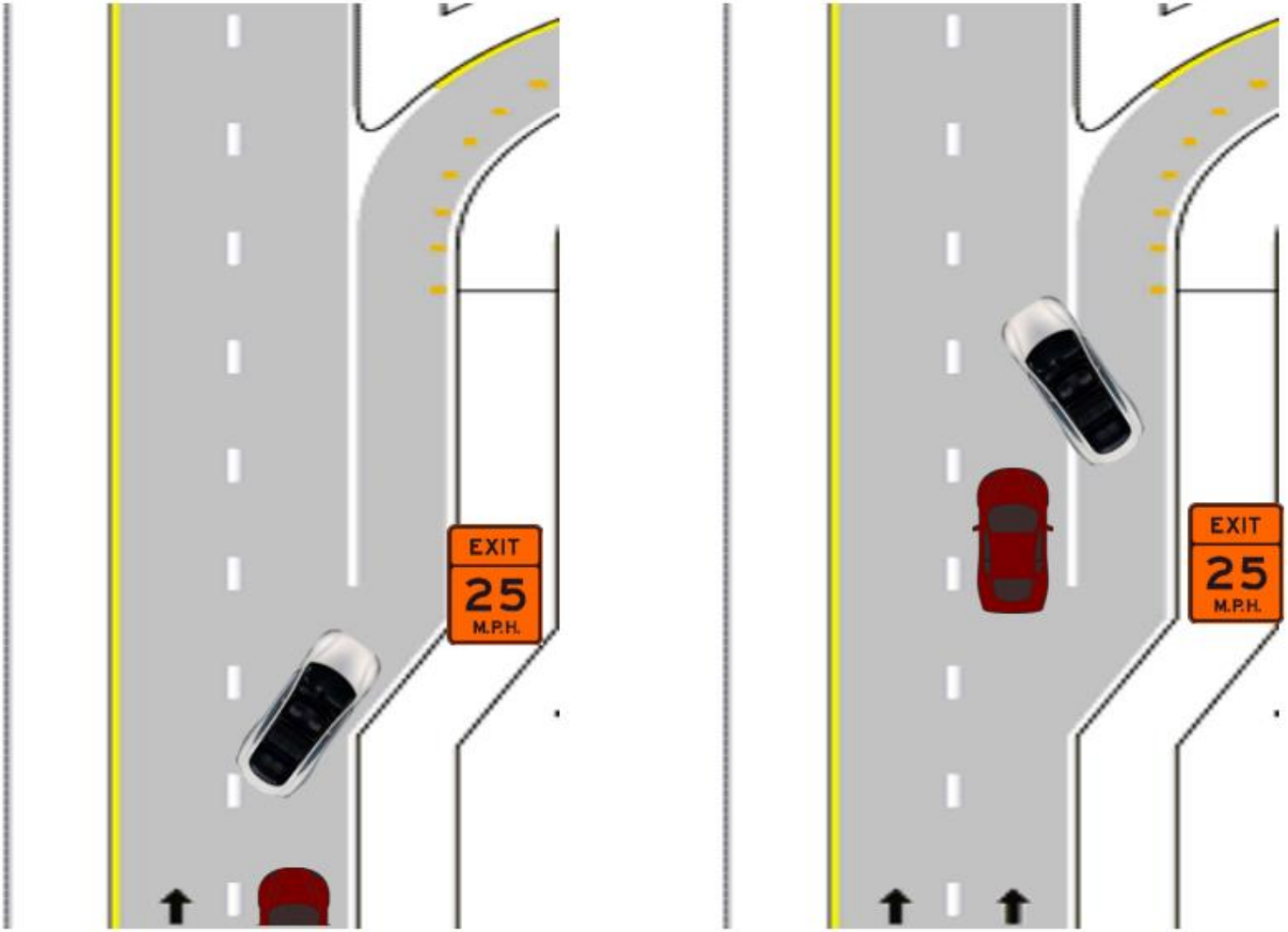
	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Steering Command		UCA-2: Driver provides unsafe steering override cmds when autopilot is engaged [L-1,L-2]		

Step 4: Potential causes of UCAs



Scenario #2

UCA-2: Driver provides unsafe steering override commands when autopilot is engaged



Spring 2016 Student project: Diogo Castilho, Megan France